Zur Theorie der identischen Kongruenzen mit Idealmoduln.

(Zweite Mitteilung.)

Von László Zányi in Szeged.

1. Es soll gezeigt werden, daß die Methoden der ersten Mitteilung[1]) zu weiteren Resultaten führen.

Es sei wieder $f(x)$ eine ganze rationale Funktion, deren Koeffizienten auch Unbestimmte oder ganze rationale Funktionen von Unbestimmten mit ganzen Koeffizienten aus einem Körper $\mathfrak{K}$ sein können. Wir wollen

$$\prod_{\tau_a} f(x+(\tau_a \pi)^n) \qquad (\mathrm{mod}\ \mathfrak{p}^{a+1})$$

berechnen.[2]) Wie in der ersten Mitteilung, erhält man

$$(42)\quad \begin{cases} \displaystyle\prod_{\tau_a} f(x+(\tau_a\pi)^n) \equiv \prod_{\tau_{a-1}} \prod_{\tau} f(x+(\tau_{a-1}+\pi^{a-1}\tau)^n \pi^n) \equiv \\ \displaystyle\qquad \equiv \prod_{\tau_{a-1}} f(x+(\tau_{a-1}\pi)^n)^{N(\mathfrak{p})} + \\ \displaystyle + n\pi^{a+n-1} \prod_{\tau_{a-1}} f(x+(\tau_{a-1}\pi)^n)^{N(\mathfrak{p})} \cdot \sum_{\tau_{a-1}} \tau_{a-1}^{n-1} \frac{f'(x+(\tau_{a-1}\pi)^n)}{f(x+(\tau_{a-1}\pi)^n)} \cdot \sum_{\tau} \tau \\ \qquad\qquad\qquad\qquad\qquad\qquad (\mathrm{mod}\ \mathfrak{p}^{a+n}). \end{cases}$$

Ist daher $N(\mathfrak{p})>2$, $a>1$ oder $N(\mathfrak{p})=2$, $n>1$, $a>1$, oder endlich $N(\mathfrak{p})=2$, $n=1$, $a>2$, dann wird

$$(43)\qquad \prod_{\tau_a} f(x+(\tau_a\pi)^n) \equiv \prod_{\tau_{a-1}} f(x+(\tau_{a-1}\pi)^n)^{N(\mathfrak{p})} \qquad (\mathrm{mod}\ \mathfrak{p}^{a+1}).$$

Betrachten wir zunächst die Fälle $N(\mathfrak{p})>2$, oder $N(\mathfrak{p})=2$, $n>1$. Es ist

---

[1]) *Diese Acta,* **5** (1931), S. 117—131.

[2]) Wie man aus der Rechnung sieht, kann man im Falle $n>1$ schärfere Resultate erzielen, wir gehen jedoch hierauf nicht ein.

$$\prod_\tau f(x+(\tau\pi)^n) \equiv \prod_\tau \left(f(x)+\tau^n\pi^n f'(x)\right) \equiv$$
$$\equiv f(x)^{N(\mathfrak{p})} + \pi^n f(x)^{N(\mathfrak{p})-1} f'(x) \sum_\tau \tau^n \equiv f(x)^{N(\mathfrak{p})} \pmod{\mathfrak{p}^2},$$

daraus folgt

$$\prod_{\tau_a} f(x+(\tau_a\pi)^n) \equiv f(x)^{N(\mathfrak{p}^a)} \pmod{\mathfrak{p}^{a+1}}. \tag{44}$$

Es sei nun $N(\mathfrak{p})=2$, $n=1$. Zunächst wird

$$\prod_\tau f(x+\tau\pi) \equiv f(x)f(x+\pi) \pmod{\mathfrak{p}^2}, \tag{45}$$

ferner ist

$$\prod_{\tau_2} f(x+\tau_2\pi) \equiv f(x)f(x+\pi)f(x+\pi^2)f(x+\pi+\pi^2) \pmod{\mathfrak{p}^3}.$$

Da

$$f(x+\pi^2)f(x+\pi+\pi^2) \equiv \left(f(x)+\pi^2 f'(x)\right)\left(f(x+\pi)+\pi^2 f'(x+\pi)\right) \equiv$$
$$\equiv f(x)f(x+\pi)+\pi^2\left(f(x+\pi)f'(x)+f(x)f'(x+\pi)\right) \equiv$$
$$\equiv f(x)f(x+\pi)+2\pi^2 f(x)f'(x) \equiv f(x)f(x+\pi) \pmod{\mathfrak{p}^3}$$

ausfällt, wird

$$\prod_{\tau_2} f(x+\tau_2\pi) \equiv f^2(x)f^2(x+\pi) \pmod{\mathfrak{p}^3}. \tag{46}$$

Es sind jetzt zwei Fälle zu unterscheiden.

1. Im Falle $N(\mathfrak{p})=2$, $n=1$, $\mathfrak{p}^2 \nmid 2$, kann $\pi=2$ gesetzt werden und wir bekommen

$$\prod_{\tau_a} f(x+\tau_a\pi) \equiv \left(f(x)f(x+2)\right)^{\frac{N(\mathfrak{p}^a)}{2}} \pmod{\mathfrak{p}^{a+1}}. \tag{47}$$

2. Im Falle $N(\mathfrak{p})=2$, $n=1$, $\mathfrak{p}^2 | 2$, wird

$$\prod_{\tau_2} f(x+\tau_2\pi) \equiv f^2(x)\left(f^2(x)+\pi^2 f'^2(x)\right) \pmod{\mathfrak{p}^3},$$
$$\prod_{\tau_3} f(x+\tau_3\pi) \equiv f^4(x)\left(f^2(x)+\pi^2 f'^2(x)\right)^2 \equiv f^8(x) \pmod{\mathfrak{p}^4}$$

und

$$\prod_{\tau_a} f(x+\tau_a\pi) \equiv f(x)^{N(\mathfrak{p}^a)} \pmod{\mathfrak{p}^{a+1}}, \quad a>2. \tag{48}$$

Diese Formel hat die Gestalt von (44), jedoch kann sie auch auf die Form von (47) gebracht werden. Es ist nämlich in unserem Falle

$$f(x) \equiv f(x+2) \pmod{\mathfrak{p}^2}, \ldots, (f(x))^{2^{a-1}} \equiv (f(x+2))^{2^{a-1}} \pmod{\mathfrak{p}^{2+2(a-1)}}$$

und da $2a > a+1$ ausfällt, wird

$$\prod_{\tau_a} f(x+\tau_a\pi) \equiv \left(f(x)f(x+2)\right)^{\frac{N(\mathfrak{p}^a)}{2}} \pmod{\mathfrak{p}^{a+1}}, \quad a>2. \tag{48*}$$

2. Analog kann

$$\prod_{\varkappa_a} f(x+(\varkappa_a \pi)^n) \qquad (\mathrm{mod}\ \mathfrak{p}^{a+1})$$

berechnet werden. Es wird im Falle $N(\mathfrak{p})>2$, oder $N(\mathfrak{p})=2$, $n>1$,

$$\prod_{\varkappa_a} f(x+(\varkappa_a \pi)^n) \equiv f(x)^{\varphi(\mathfrak{p}^a)} \qquad (\mathrm{mod}\ \mathfrak{p}^{a+1}). \tag{49}$$

Ist $N(\mathfrak{p})=2$, $n=1$, so wird zunächst

$$\prod_{\varkappa} f(x+\varkappa\pi) \equiv f(x+\pi) \qquad (\mathrm{mod}\ \mathfrak{p}^2),$$

$$\prod_{\varkappa_2} f(x+\varkappa_2\pi) \equiv f(x+\pi) f(x+\pi+\pi^2) \qquad (\mathrm{mod}\ \mathfrak{p}^3).$$

Es sind zwei Fälle zu unterscheiden.

1. $N(\mathfrak{p})=2$, $n=1$, $\mathfrak{p}^2 \nmid 2$. Man kann $\pi=2$ setzen und es wird

$$\prod_{\varkappa_a} f(x+\varkappa_a\pi) \equiv (f(x+2) f(x+6))^{\frac{\varphi(\mathfrak{p}^a)}{2}} \qquad (\mathrm{mod}\ \mathfrak{p}^{a+1}), \qquad a>1. \tag{50}$$

2. $N(\mathfrak{p})=2$, $n=1$, $\mathfrak{p}^2 | 2$. Da in diesem Falle

$$f(x+\pi) f(x+\pi+\pi^2) \equiv f(x+\pi)(f(x+\pi)+\pi^2 f'(x+\pi)) \equiv$$
$$\equiv f^2(x+\pi)+\pi^2 f(x+\pi) f'(x) \equiv (f(x)+\pi f'(x))^2+\pi^2 f(x) f'(x) \equiv$$
$$\equiv f^2(x)+\pi^2 (f'^2(x)+f(x) f'(x)) \qquad (\mathrm{mod}\ \mathfrak{p}^3),$$

$$\prod_{\varkappa_3} f(x+\varkappa_3\pi) \equiv (f^2(x)+\pi^2(f'^2(x)+f(x)f'(x)))^2 \equiv f^4(x) \qquad (\mathrm{mod}\ \mathfrak{p}^4)$$

ausfällt, so wird

$$\prod_{\varkappa_a} f(x+\varkappa_a\pi) \equiv f(x)^{\varphi(\mathfrak{p}^a)} \qquad (\mathrm{mod}\ \mathfrak{p}^{a+1}),\ a>2. \tag{51}$$

Diese Formel hat die Gestalt der Formel (49). Man kann zeigen, daß sie auch auf die Form von (50) gebracht werden kann. Es ist nämlich in unserem Falle

$$f(x) \equiv f(x+2) \equiv f(x+6) \ (\mathrm{mod}\ \mathfrak{p}^2), \ldots,$$
$$(f(x))^{2^{a-2}} \equiv (f(x+2))^{2^{a-2}} \equiv (f(x+6))^{2^{a-2}} \qquad (\mathrm{mod}\ \mathfrak{p}^{2a-2})$$

und daraus folgt unsere Behauptung, weil $2a-2 \geqq a+1$ ausfällt.

3. Die auf der letzten Seite der ersten Mitteilung angestellten Überlegungen bedürfen einer Berichtigung; man ersetze S. 131 durch den folgenden Wortlaut:

„Wenn $\prod_{\varkappa_a} f(\varkappa_a^n) \not\equiv 0 \pmod{\mathfrak{p}}$ ist, erhält man durch Division

$$\prod_{\tau_{a-1}} f((\tau_{a-1}\pi)^n) \equiv f(0)^{N(\mathfrak{p}^{a-1})} \pmod{\mathfrak{p}^a},\ N(\mathfrak{p}) > 2.$$

Es sei jetzt

$$f(x) = F(y-c+x) = \alpha_m(y-c+x)^m + \ldots + \alpha_1(y-c+x) + \alpha_0,$$

wo $\alpha_m, \ldots, \alpha_1, \alpha_0, c$ ganze Zahlen des Körpers $\mathfrak{K}$ bedeuten. Man sieht, daß $f(\varkappa_a^n) \equiv 0 \pmod{\mathfrak{p}}$ nur im Falle eintritt, wenn $f(0) = F(y-c) \equiv 0 \pmod{\mathfrak{p}}$ ausfällt. Also ist im Falle $F(y-c) \not\equiv 0 \pmod{\mathfrak{p}}$

$$\prod_{\tau_{a-1}} F(y-c+(\tau_{a-1}\pi)^n) \equiv F(y-c)^{N(\mathfrak{p}^{a-1})} \pmod{\mathfrak{p}^a},\ N(\mathfrak{p}) > 2.$$

Diese Kongruenz ist jedoch auch im Falle $F(y-c) \equiv 0 \pmod{\mathfrak{p}}$ gültig und enthält den Lubelskischen Satz."

Endlich sollen noch einige Verbesserungen an der ersten Mitteilung angebracht werden.

S. 119, letzte Zeile „und zu $\frac{\mathfrak{a}}{\mathfrak{p}^a}$ teilerfremde" ist zu streichen.

S. 122, Zeile 9 statt „Zahl" zu lesen „Form."

S. 124, in den Formeln (19) und (20) statt $\mathfrak{p}$ zu lesen $\mathfrak{p}^a$.

S. 124, Zeile 17 und S. 128, Zeile 10 statt $l_i = \frac{\varphi(\mathfrak{p}_i)}{n}$ zu lesen $l_i = \frac{\varphi(\mathfrak{p}_i)}{d_i}$.

S. 125, nach Formel (29) und S. 126, nach Formeln (34) und (37) einzuschalten: „ist noch $\mathfrak{p}^2 | 2$, so wird."

S. 127, Zeile 19 „der Wahl von" ist zu streichen.

S. 128, die 3 letzten Zeilen sind zu streichen.

S. 129, Zeile 5 ist einzuschalten: „im Falle $l_i > 1$", Zeile 7 ist einzuschalten: „im Falle $l_i = 1$, $A_0 = x - 1$", Zeile 8 ist das Vorzeichen zu streichen, Zeile 17 nach $a_i > 3$ ist einzuschalten: „$\mathfrak{p}^2 \nmid 2$, $a_i = 1$," Zeile 6 von unten ist einzuschalten: „wie eine leichte Rechnung zeigt."

S. 130, statt $(x^2-1)^{\frac{a}{2}}$ zu lesen $(x^2-x)^{\frac{a}{2}}$.

Die Rechnungen in der ersten Mitteilung können etwas abgekürzt werden. Die Formeln (9) und (10) sind im Falle $N(\mathfrak{p}) = 2$, n gerade schon für $a > 1$ gültig, wie dies aus (7) ersichtlich ist.

(Eingegangen am 2. November 1931.)